

1011105

# (12) UK Patent Application (19) GB (11) 2 364 142 (13) A

(43) Date of A Publication 16.01.2002

(21) Application No 0015821.2

(22) Date of Filing 28.06.2000

(71) Applicant(s)

Robert Morris

54 Beaufort Road, ASHTON-UNDER-LYNE, Lancs,  
OL6 6NU, United Kingdom

(72) Inventor(s)

Robert Morris

(74) Agent and/or Address for Service

Robert Morris

54 Beaufort Road, ASHTON-UNDER-LYNE, Lancs,  
OL6 6NU, United Kingdom

(51) INT CL<sup>7</sup>

G06F 1/00 , H04L 12/58

(52) UK CL (Edition T )

G4A AAP

H4K KF50X KOD4

(56) Documents Cited

None

(58) Field of Search

UK CL (Edition S ) G4A AAP

INT CL<sup>7</sup> G06F 1/00

Online: WPI,EPODOC,JAPIO,TDB,INSPEC

(54) Abstract Title

Detection of an email virus by adding a trap address to email address lists

(57) The address of a virus notification program on a email server is added to the address book of all computers covered by the detection service. When an email virus is active, it propagates by sending further emails to all addresses in the infected computer's email address book. If the virus notification program receives an email at this address then it concludes that a virus is active and warns the user or administrator. The server may halt the transmission of all email messages from the local network. Outgoing messages may be queued for a short time so that their transmission can be halted when a virus is detected. The virus notification program may be located at an internet site.

GB 2 364 142

## Description

### An email virus notification system

#### Field

This invention relates to the detection of a computer virus which propagates through email

#### Background

An address book, in the context of email software, is a list of persons, together with their email addresses, kept by the email program to enable the user to send messages to these persons without having to memorise or independently keep a record of their addresses.

An email virus is a computer program which, once it has taken control of the user's computer, sends a copy of itself to those addresses listed in the address book, without the user's consent, in order to propagate itself. In many cases the virus will then go on to cause malicious damage to the computer system.

#### Essential Features

The present invention provides the user (or a nominated other person, Eg computer system administrator) with a warning that a virus has propagated itself using the user's address book, or, in some implementations, could be used to prevent the email messages containing the virus from leaving the local network on which the infected computer is located, and hence halt the propagation of the virus.

In order for this invention to function, a computer program must be written and installed on a mail server computer, which will respond to any messages it receives by sending out a warning message, or taking other action (such as that described in Example 2 below). The exact address assigned to the program is unimportant, so long as it is not used for any other purpose.

The users who wish to be covered by the invention then add this address to their email address book. In the event of an email virus infecting their computer, the virus will send a copy of itself to, amongst others, the program mentioned above, which will result in a warning message being issued, or other action being executed.

### **Example 1**

The following is a description of the invention used as an email virus notification system provided as a public service on the Internet.

A server computer on the Internet is set up with a program containing the invention. Upon joining the service, users are instructed to put this program's email address in their email address book, as previously discussed. When the program is triggered by the receipt of an email from a virus, it sends an email message back to the user (or a person nominated by the user when they joined the service) warning them of the presence of a virus in their email system.

### **Example 2**

The following is a description of the invention used as an email virus notification and propagation prevention system in a local area network (LAN) environment.

It is industry standard practice for a series of computers within an organisation to be connected together on a LAN, and for all email messages sent from these computers to be sent via a server computer on the LAN (and not directly to the recipient). In this environment, the invention would function as a warning system in the same manner as described above, but in addition could be used to prevent propagation of the virus.

The mail server computer, through which all email messages from any of the computers on the LAN must pass, is set up to store outgoing messages in a queue for a short time (perhaps only a few minutes) before sending them on to their destination. When the program containing the invention, running on this server, is triggered, it temporarily disables the delivery of messages in the queue, and informs the system administrator of the presence of the virus. The system administrator can then check the messages in the queue, and remove any copies of the virus contained therein, thus preventing propagation of the virus. Thereafter the system administrator would reset the mail server to normal operation.

## **Claims**

### **An email virus notification system**

1. An email virus notification system which triggers on receipt of an email message delivered to its address, where that email address has been listed in the email address book on those computers which are being covered by the virus notification system.
2. An email virus notification system as claimed in Claim 1, where upon being triggered an email message is sent back to the user to inform them of the presence of the virus.
3. An email virus notification system as claimed in Claim 1, where upon being triggered an email message is sent to a system administrator or other nominated person to inform them of the presence of the virus.
4. An email virus notification and propagation prevention system as claimed in Claim 1, where upon being triggered the program stops email messages queued for delivery from being sent, and alerts the system administrator or other personnel (by email or any other means), so as to enable this person to remove the virus and thereby halt its propagation.
5. An email virus notification system implemented substantially in the manner described in Example 1 herein.
6. An email virus notification and propagation prevention system implemented substantially in the manner described in Example 2 herein.



Application No: GB 0015821.2  
Claims searched: 1-6

Examiner: Keith Sylvan  
Date of search: 22 June 2001

**Patents Act 1977**  
**Search Report under Section 17**

**Databases searched:**

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): G4A (AAP)

Int Cl (Ed.7): G06F (1/00)

Other: Online: WPI,EPODOC,JAPIO,INSPEC,TDB

**Documents considered to be relevant:**

Category	Identity of document and relevant passage	Relevant to claims
	NONE	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

**THIS PAGE BLANK (USPTO)**